How AV Detection Works ?

Signature-Based Detection

- AVs maintain a database of known malware signatures or hashes.
- When scanning a file, the AV calculates its signature/hash and compares it against the database.
- If a match is found, the file is flagged as malicious based on the known signature.
- This method is effective for detecting previously identified malware variants.

Heuristic Analysis

- AVs use heuristic rules to analyze files for suspicious characteristics like rare instructions, junk code, or packing/obfuscation.
- Even without an exact signature match, if enough suspicious traits are present, the file may be flagged as potential malware.
- Heuristics help detect new or modified malware that lacks a known signature.

Behavioral Monitoring

- AVs monitor the behavior of running processes, looking for malicious actions like code injection, keylogging, or modifying system files.
- Suspicious behaviors exhibited during execution can indicate the presence of malware, even without a known signature.
- This approach is similar to Host-based Intrusion Prevention Systems (HIPS).

Memory Scanning

- Some AVs scan the memory of running processes to detect malicious code loaded in memory.
- This can catch fileless malware that resides only in memory without being written to disk.
- Memory scanning is a more resource-intensive operation compared to file scanning.

Cloud-Based Detection

- AVs can submit suspicious files or behaviors to a cloud-based analysis engine for further inspection.
- The cloud engine correlates data from multiple endpoints to identify new malware patterns and techniques.
- This allows individual endpoints to benefit from the collective intelligence of the AV vendor's user base.